基于范畴论的业务目标模型形式化 *

李宗花 [1,2]，李必信 [2]

(1. 淮阴师范学院 计算机科学与技术学院，江苏 淮安 223300; 2. 东南大学 计算机科学与工程学院，南京 211189)

摘　要：面向目标需求语言模型（goal-oriented requirement language，GRL）聚焦于待定的需求，被广泛地应用于业务系统的初始需求建模，其模型的正确性影响到业务系统的开发质量。鉴于业务目标模型的形式化可以验证模型的正确性，提出了一种利用范畴论形式化 GRL 模型的方法。首先，依据 GRL 元模型结构，应用范畴论中的态射机制形式化描述 GRL 模型中目标与目标、目标与任务以及任务与任务等节点之间的关系；然后，通过增加范畴模型中的初始对象和终止对象，设计紧邻序列来表示多个目标与任务实施的因果关系；最后，设计业务目标模型系统的正确性结构性质。应用 Web Payment 系统实验表明，形式化业务范畴模型能够验证 GRL 模型的正确性，提高目标建模的质量。

关键词：GRL 模型；范畴论；模型形式化；模型正确性验证

中图分类号：TP311　　doi: 10.19734/j.issn.1001-3695.2018.10.0822

To formalize business goal model based on category theory

Li Zonghua[1, 2], Li Bixin[2]

(1. *School of Computer Science & Technology*, *Huaiyin Normal University* 223300 *Huaian*, *Jiangsu*, *China*; 2. *School of Computer Science & Engineering*, *Southeast University* 211189 *Nanjing*, *Jiangsu*, *China*)

Abstract: The Goal-Oriented Requirement Language (GRL) focuses on the undetermined requirement, which has been widely used to capture initial requirement of the business system. The correctness of the GRL model is a key to influencing the development quality of the business system. Based on graph category, this paper proposes a model formalization approach to verify the correctness of the GRL model. Firstly, according to the meta-model of the GRL model, the morphism mechanism of the category theory has been applied to describe the relationship between goal node and task node, one goal node and the other goal node, one task node and the other task node. Then, the initial object and terminal object of the category model were added, and the neighborhood sequence was designed to represent the causation between the multiple goals and the task implementations. Finally, the correctness structure properties of the business objective model system were designed. The Web Payment system was applied to demonstrate the result of the formalization analysis and correctness verification. It shows that the graph category model can verify the correctness of GRL model and improve the quality of goal modeling.

Key words: GRL model; category theory; model formlization; model correctness verification

0　引言

对于业务系统来说，捕获明确清晰的业务目标是至关重要的，因而业务目标模型是否合适、完整、清晰或一致对于软件的质量有着重要的影响[1]。面向目标的需求工程（goal-oriented requirement engineering，GORE）认为业务系统及其环境是一个活动组件的集合，活动组件可以约束他们的行为，从而保证其任务的强制实施[2,3]。面向目标需求语言（GRL）作为一种支持面向目标建模的语言[4,5]，聚焦于待定的需求分析，由 Osis 团队开发并用于获取业务系统的目标、实现目标的可选择方案制定以及确定目标贡献值的大小[2,7]。GRL 模型可有效的定义系统初始问题，被广泛的应用于业务系统的初始需求建模[1,6,8]。

GRL 语言允许业务分析员和开发者以图标记的方式描述业务系统的目标、任务、软目标等信息。但其标记描述[4]并未包括完整的目标模型语义[9]，使得 GRL 模型的正确性难以验证[10]。由于目标模型所具有的约束关系可以处理业务目标之间的相互关系，Popova 等人[11]提出了一个面向目标方法的完整形式化框架，该形式化框架利用谓词语言（predicate language）形式化目标模型中的 hard 目标、soft 目标、目标约束、目标分解以及目标细化等。Giachetti 等人[12]应用模型驱动方法设计特定的对象约束语言(object constraint language, OCL)规则对目标需求模型进行验证。Mendonça 等人[13]基于上下文形式化方法提出了面向目标的依赖分析框架，以帮助专家在不同的上下文中评估设计与运行时的可靠性。Diamantini 等人[14]设计了基于本体的目标建模方法。这些形式化方法能有效的形式化目标模型的元素，验证目标模型的正确性。但对目标节点之间的关系刻画还略显不足。

范畴论是以抽象方法描述数学结构和表示结构之间的相互关系[15]。利用"物件"和"态射"来形式化某个特定的范畴，范畴论可用于不同领域结构的发现和验证连接[16]。在软件工程领域，研究者利用范畴论对软件体系结构进行形式化分析

收稿日期：2018-10-29；**修回日期：**2018-12-29　**基金项目：**江苏省高校自然科学研究面上项目（18KJB520006）；国家自然科学基金资助项目（41471425）；淮安市科技计划资助项目（HABZ201701）

作者简介：李宗花（1981-），女，副教授，博士，主要研究方向为形式化方法和模型驱动开发（leeleaf@163.com）；李必信（1969-），男，教授，博士，主要研究方向为智能化软件工程.

[17~19]。因此，本文利用范畴论在描述结构方面的优势，形式化业务目标模型，利用“态射”刻画各业务目标节点之间的关系，进而验证目标模型的正确性。

1　GRL 模型

GRL 可以标志出利益相关者（参与者）和他们的目的（目标，任务和软目标），以及用图的方式识别功能需求（目标，任务）和非功能需求（软目标）[20]，其元模型结构如图 1 所示。GRL 的重点在于初始业务目标的提取，即从不同的终端用户和业务协作者的角度出发，提取出每一个参与者的业务目标，然后再分析这些业务目标之间的关联关系[21]。

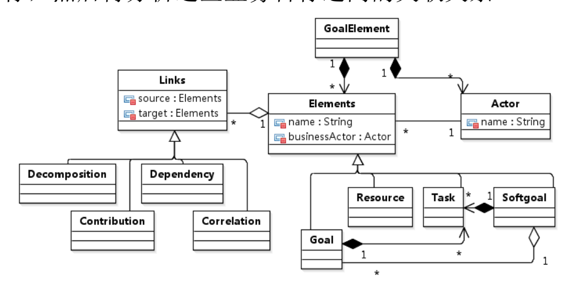


图 1　GRL 元模型

Fig. 1　GRL Meta model

GRL 基本的模型元素如图 2 所示。可以看出，GRL 由意图元素（intentional elements）、意图关系（intentional relationships）和参与者（actor）三类组成。其中意图元素包括目标（goal）、任务（task）、软目标（softgoal）、想法和资源（resource）；意图关系包括分解关系（decomposition）、贡献关系（contribution）、关联关系（correlation）和依赖关系（dependency）。这些意图元素和意图关系用于允许回答问题的模型，比如为什么特定的行为、信息和结构被选为描述系统需求以及什么选择方案需要考虑，使用何种标准审议备选方案以及什么原因选择其中一个选择项等。因此，可以认为 GRL 模型由参与者、参与者所需要完成的目标或任务集合以及链接元素组成。

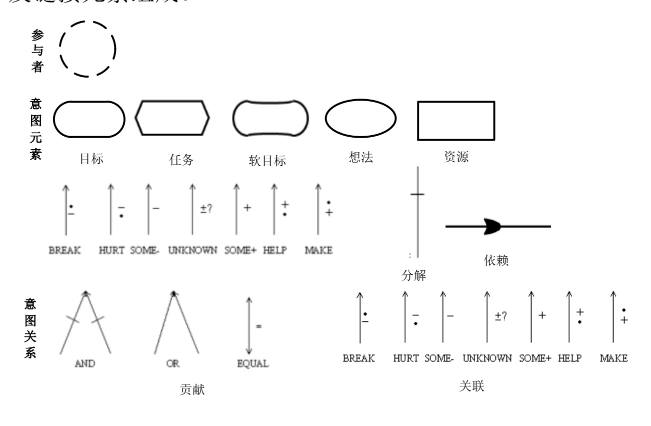


图 2　基本的 GRL 元素

Fig. 2　Basic GRL elements

2　业务目标模型的形式化

由于目标模型系统一定存在初始点目标对象和终点目标对象。因此，本文的理论关键在于范畴模型中的初始目标(*initial*)对象和终止目标(*terminal*)对象的确定。其形式化的描述为：假设一个 *initial* 对象 *I* 存在于范畴 *C* 中，而范畴 *C* 中除了对象 *I* 之外的每一个对象一定是某个特定态射的余论域(*codomain*)，而对象 *I* 只是某个态射的论域(*domain*)，即范畴 *C* 中存在一个对象 *X*，对象 *I* 与对象 *X* 之间存在独一无二的射 $I \to X$，因此，可认为对象 *I* 是范畴 *C* 的初始目标对象。假设一个 *terminal* 对象 *T* 存在于范畴 *C* 中，而范畴 *C* 中除了对象 *T* 之外的每一个对象一定是某个特定态射的论域，而对象 *T* 只是某个态射的余论域，即范畴 *C* 中存在一个对象 *X*，对象 *X* 与对象 *T* 之间存在独一无二的射 $X \to T$，因此，可认为对象 *T* 是范畴 *C* 的终点目标对象。初始对象与终止对象的确定有利于完整的形式化描述业务目标模型。

定义 1　基于范畴论理论，一个系统的业务目标图可以定义为一个函数

$$F: E \to V \times V$$

其中：*E* 是边的集合，*V* 是节点集合，令 $e \in E$，则 $F(e)$ 的值是一个序对 (n_0, n_1)，其中 n_0 表示为 *e* 的源节点，n_1 表示为 *e* 的目标节点，即 $dom(e) = n_0, cod(e) = n_1$。令 $C = (C_A, C_N)$ 表示为集合的序对，C_A 表示为射字符集合（arrow 集合），而 C_N 表示为节点字符的集合（object 集合），则一个业务目标图可以定义为一个系统[22]，即

$$G = (A, G_A, G_N, s, t, m_a, m_n),$$

其中：*A* 表示 actor，即目标系统中的参与者对象，对应业务系统中的业务参与者。

G_A 表示射的集合，$\forall a_i$，$a_i \in G_A$，则 $a_i ::= a_{dc} \mid a_c \mid a_{dp}$。其中 a_{dc} 代表射的类型为“*Decomposition*”，表示将业务目标节点分解为若干个业务任务节点；a_c 代表射的类型为“*Contribution*”，表示某个任务节点贡献于其他任务节点或者目标节点；a_{dp} 代表射的类型为“*Dependency*”，表示某个任务节点与其他任务节点或目标节点存在依赖关系。

G_N 表示节点的集合，对应业务系统中的业务服务或业务活动。$\forall n_i$，$n_i \in G_N$，则 $n_i = (n_{name}, n_{type})$，其中 n_{name} 表示节点的名称，n_{type} 表示节点的类型，$n_{type} ::= ng \mid nt \mid nsg \mid nr$。$ng$ 表示节点类型为“goal”，表示业务系统中的功能性目标，对应业务服务概念；nt 表示节点类型为“task”，对应业务任务概念；nsg 表示节点类型为软目标，描述业务系统中非功能性方面的需求；nr 表示节点类型为“resource”，表示业务系统中实现业务目标所需的相关资源。这些节点往往属于某个参与者组件，因此，每个参与者对应一个节点集合。

$s: G_A \to G_N$ 表示源映射。

$t: G_A \to G_N$ 表示目标映射。

$m_a: G_A \to C_A$ 表示射字符集的映射。

$m_n: G_N \to C_N$ 表示节点字符集的映射。

因此，目标模型系统可以表示为

$$G: C_A \xleftarrow{m_a} G_A \underset{t}{\overset{s}{\rightrightarrows}} G_N \xrightarrow{m_n} C_N$$

几点说明：

a)若 $G_N = \varnothing$，则 $G = <\varnothing, \varnothing, \varnothing, \varnothing, \varnothing, \varnothing, \varnothing>$，此时称 G 为空的目标模型系统。

b)若 $G_A = \varnothing$，则 $G = <A, \varnothing, G_N, \varnothing, \varnothing, \varnothing, \varnothing>$，此时称 G 为空的离散目标模型系统。

c)若 G_N 和 G_A 均为有穷集合，则称 G 为有穷目标模型系统。

d)若 $\forall n_0, n_1, n_2, n_3, n_4, \ldots, n_i \in G_N$，存在序对 (n_0, n_1)，(n_1, n_2)，(n_2, n_3)，. . .，(n_{i-1}, n_i)，且序对为有穷集合，则称 G 为局部目标模型系统。

e)若 $\forall n_0, n_1, n_2, n_3, n_4, \ldots, n_i \in G_N$，存在唯一序对 (n_0, n_i)，且 $\forall f \in G_A$，$\exists s(f) \neq t(f)$，则称 G 为简单目标模型系统。

f) $s(f) = ng1$ 表示态射 *f* 的源节点为 $ng1$，$t(f) = ng2$ 表示态射 *f* 的目标节点为 $ng2$。

根据以上六点说明可知：

a)离散目标模型系统为简单目标模型系统。

b)简单目标模型系统为局部目标模型系统。

c)每一个射（箭头）都有唯一的源节点和唯一的目标节点。

根据以上定义和说明，则有：

定理 1　设 G 为目标模型系统，且 $ng1, ng2, ng3 \in G_N$，若存在射 f：$ng1 \to ng2$，且射 g：$ng2 \to ng3$，则射 $g \circ f$：$ng1 \to ng3$。

证明　若存在射 f：$ng1 \to ng2$ 且射 g：$ng2 \to ng3$，则

$$s(f) = ng1, t(f) = s(g) = ng2 \text{ 且 } t(g) = ng3,$$

且有

$$s(g \circ f) = s(f) = ng1 \text{ 且 } t(g \circ f) = t(g) = ng3,$$

所以有射 $g \circ f$：$ng1 \to ng3$。

定义 2　对于任意目标模型系统 G，存在射 $f: ng1 \to ng2$，假如 G 中同时也存在射 $g: ng2 \to ng1$，则

a）$s(f) = t(f) = ng1$ 且 $s(g) = t(g) = ng2$。

b）$g \circ f = 1_{ng1}$ 且 $f \circ g = 1_{ng2}$。

可以写作为 $g = f^{-1}$。称为 ng1 **同构**于 ng2，记为 $ng1 \cong ng2$。

定义 3　对于任意目标模型系统 $G =< A, G_A, G_N, s, t, m_a, m_n >$ 和 $G' =< A', G_A', G_N', s', t', m_a', m_n' >$ 满足以下条件：

a）$f \circ g = 1_{ng2}$　$A' \subseteq A$，$G_A' \subseteq G_A$ 且 $G_N' \subseteq G_N$。

b）若 $\forall ng_i \in G_N'$，则 G 和 G' 关于 ng_i 的态射相同。

c）$s' \subseteq s, t' \subseteq t$。

则称 G' 为 G 的子目标模型系统，记为 $G' \subseteq G$。

若 $G' \subseteq G$ 且 $G' \neq G$，则称 G' 为 G 的**真子目标模型系统**，记为 $G' \subset G$。若 $G' \subseteq G$ 且 $G_N' = G_N$，则称 G' 为 G 的**宽子目标模型系统**。若 $G' \subseteq G$，且当 $ng1, ng2 \in G_N'$ 时皆有 $f': ng1 \to ng2, f: ng1 \to ng2 \Rightarrow f' = f$，则称 G' 为 G 的**完全子目标模型系统**。

因此，一个子目标模型系统具有与父目标模型系统相同的语义，是父目标模型系统的中一个目标节点。该子目标模型系统是独立的、可重用的。

定义 4　对于任意目标模型系统 $G =< A, G_A, G_N, s, t, m_a, m_n >$，有 $ng1 \in G_N$，

a）若每一个 $G_{Ai} \in G_A$，$\exists t(G_{Ai}) \neq ng1$，则称 $ng1$ 为目标模型系统 G 的初始对象。

b）若每一个 $G_{Ai} \in G_A$，$\exists s(G_{Ai}) \neq ng1$，则称 $ng1$ 为目标模型系统 G 的终止对象。

c）若 $ng1$ 既是初始对象，又是终止对象，则称 $ng1$ 为零对象。

定义 5　对于任意目标模型系统 $G =< A, G_A, G_N, s, t, m_a, m_n >$，$\exists a_0 \in G_A$，且 $a_0 \subset adp$，若 $s(a_0) = ng1$，$t(a_0) = ng2$，且节点 $ng1$，$ng2$ 的 $n_{type} = gn$，则定义节点 $ng1$ 和 $ng2$ 之间需要添加一条临时射 $a_1: ng2 \to ng1$，表明节点 $ng1$ 和 $ng2$ 之间存在双射性质，表示为目标模型系统中使用依赖关系连接的节点属于不同的参与者，目标节点任务的执行结果必须要返回至源节点任务。

该定义如图 3 所示，表明节点 A、B、C 属于不同的参与者，节点 A 与节点 B 之间存在依赖关系 $adp1$，因此节点 B 执行的结果一定要返回给节点 A；同时节点 C 与节点 B 之间存在依赖关系 $adp2$，那么节点 C 的执行结果一定要返回给节点 B；根据定理 1，表明节点 A 与节点 C 之间也存在依赖，因此存在射 $adp1 \circ adp2$，其节点 C 的执行结果最终要返回给节点 A。

3　GRL 模型正确性的结构性质

Popova 等人[11]认为目标模型的正确性是指验证目标模型中业务目标之间是否存在冲突问题；Giachetti 等人[12]认为目标模型的正确性是指验证业务目标和资源是否关联了参与者，以及业务任务是否关联了实体或资源。本文设计的目标模型正确性是指以形式化方式验证目标模型中不存在孤立的目标节点、不存在闭环的目标紧邻序列、以及业务目标之间有意图关系连接。

定义 6　对于任意目标模型系统 $G =< A, G_A, G_N, s, t, m_a, m_n >$，有 $a_1, a_2, a_3, \ldots, a_n \in G_A$，满足以下条件：

应用定义 4，$s(a_1)$ 为目标模型系统 G 的初始对象。

应用定义 4，$t(a_n)$ 为目标模型系统 G 的终止对象。

存在射集合 $a_1: s(a_1) \to t(a_1)$，$a_2: t(a_1) \to t(a_2)$，$a_3: t(a_2) \to t(a_3)$，…，$a_n: t(a_{n-1}) \to t(a_n)$。

则存在一个目标紧邻序列 $Neighbor\text{-}S_i = \{s(a_1) \to s(a_2) \to s(a_3) \to \ldots \to s(a_n)\}$，代表目标模型系统中一个任务的动作序列。同时存在一个紧邻序列集合 $\sum Neighbor - S = \{s(a_1), s(a_2), s(a_3), \ldots, s(a_n)\}$，表示该紧邻序列中所有节点的集合。

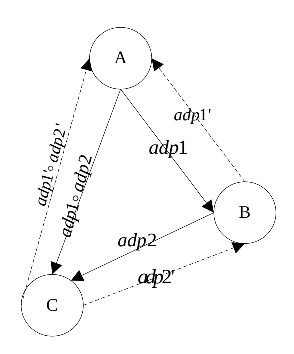


图 3　目标模型双射实例

Fig. 3　Bi-morphism instance of the goal model

定理 2　一个正确的目标模型系统是连通的。

证明　首先证明目标模型系统中的节点都不是孤立的节点，然后再证明任意节点可以从开始对象到达该节点，且该节点可到达终止对象。便可证明该模型是连通的。

对于任意目标模型系统 $G =< A, G_A, G_N, s, t, m_a, m_n >$，$\forall n_i$，$n_i \in G_N$，且根据定义 6，$n_i \in \sum Neighbor - S$，若 $\sum Neighbor - S = G_N$，表明该模型中无孤立节点，节点之间具有连通性。

定理 3　一个正确的目标模型系统是没有闭环的。

证明　对于任意目标模型系统 $G =< A, G_A, G_N, s, t, m_a, m_n >$，应用定义 4，目标模型系统 G 具有初始对象和终止对象，应用定义 6，目标模型系统 G 中的所有节点均在紧邻序列集合中，且满足定理 2，则可认为 G 是没有闭环的，表明每一条紧邻序列代表着系统中一个功能。否则，该系统没有明确的开始对象或终止对象，因而，目标系统存在闭环情况，即目标模型中至少存在一条无限循环执行的紧邻序列，表明业务系统中的目标模型是存在问题的。

定理 4　一个正确的目标模型系统应满足“目标—分派”关系。

证明　对于任意目标模型系统 $G =< A, G_A, G_N, s, t, m_a, m_n >$，假设 $ng1, nt1, nt2, nt3 \in G_N$，$ng1 = \{nt1, nt2, nt3\}$。其中，$ng1$ 表示为目标系统的一个业务目标，该目标被分解为 $nt1, nt2, nt3$ 三个子目标。在目标系统中，$ng1$ 表示为全局目标，$nt1, nt2, nt3$ 表示为局部任务，存在射 $edc1: ng1 \to nt1$，$edc2: ng1 \to nt2$，$edc3: ng1 \to nt3$。业务目标模型作为捕获业务系统的初始需求，将功能模块划分为一系列任务步骤，被分解的目标表示为全局目标。在划

分子目标时，一方面子目标之间不能产生矛盾，即一个子目标的实现不能导致其他子目标的失败（即子目标之间不能存在依赖关系，不能让一个子目标使得其他子目标的前置或后置条件不成立)；另一方面子目标与全局目标之间不能产生矛盾，全局目标实现意味着所有子目标实现，反之，只要任一子目标没有实现，则全局目标也不能实现。所以目标模型系统中的节点元素满足“目标-分配”关系。

定理 5 一个正确的子目标模型系统应与父目标模型系统具有相同的语义，不超过父目标模型系统资源使用的边界，且具有共同的软目标。

证明 对于任意目标模型系统 $G=<A,G_A,G_N,s,t,m_a,m_n>$，假设 $ng1\in G_N$，$ng1=<A',G_A',G_N',s',t',m_a',m_n'>$，则表明 ng1 是 G 的子目标模型系统，与 G 具有相同的语义。$nr\in G_N$，$nsg\in G_N$ 分别表示为目标模型系统 G 中的所有资源节点集合和所有软目标节点集合，假设 $A'\subseteq A$ 且 $G_N'\subseteq G_N$，$\forall nr_i'\in nr, nsg_i'\in nsg$，表明子目标模型系统 ng1 的系统资源不超过父目标模型系统的边界，且具有共同的软目标。

其目标模型的形式化正确性验证将结合具体的案例在第 4 节进行分析。

4 业务目标模型形式化实例分析

4.1 建模环境

本文使用的运行实例来自于 W3C 标准文档[23]中的 Web Payment 业务系统，该业务系统的场景描述如下：首先，购物者（customer）浏览网上购物网站（online shopping site）上的商品；然后，customer 选择商品并放入购物车；一旦该 customer 下订单购买该商品，该用户需要登录自己的账户，并向 online shopping site 提供自己的银行账户或其他支付信息（支付宝、谷歌钱包或者苹果支付等），同时 online shopping site 还会要求用户提供验证码等信息；online shopping site 提交用户的支付信息给相应的金融机构（financial company），customer 和 online shopping site 都能收到来自金融机构的支付凭证；最后，online shopping site 发送给 customer 数字凭证，同时 online shopping site 的发货部门会将商品发送给 customer。

4.2 业务目标建模

业务目标的建模通过以下活动完成：a）通过业务系统中关于业务需求的自然语言描述，提取和分析该业务问题描述中的名词和动词，识别业务系统的参与者和功能方面的意图元素；b）将相关意图元素归类于参与者，表明该意图元素是由某一个参与者作用并实施的；c）建立意图元素之间的意图关系。通过对 Web Payment 的场景分析，应用和实施以上 GRL 建模的三个活动，Web Payment 系统的初始目标模型如图 4 所示。该图所示的意图关系表明，顾客是否能获得好的网上购物服务完全依赖于 online shopping site 系统提供的服务。如目标“gain goods options”与任务“provide goods options”之间存在依赖关系；而 customer 与 financial company 之间的交互依赖于 online shopping site 提供的服务。

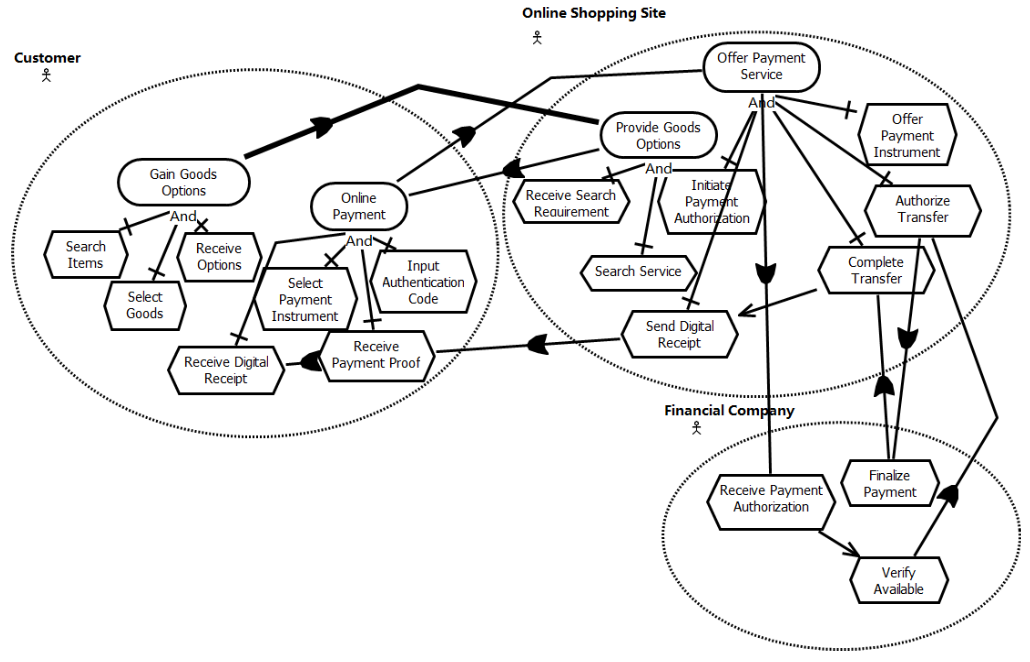


图 4 Web Payment 系统的 GRL 模型

Fig. 4 GRL model of Web Payment

4.3 业务目标模型形式化

根据定义 1 形式化 GRL 模型，图 4 所示的目标模型节点信息如表 1 所列。因此，Web Payment 业务系统的目标模型可以被图范畴定义为

$$G=(A,G_A,G_N,s,t,m_A,m_N)$$

其中参与者集合 A 为 $A=\{customer, online\ shoping\ site, financial\ company\}$，箭头字符集合为 G_A：

$$G_A=\{edc1,edc2,edc3,edc4,edc5,edc6,edc7,edc8,edc9,edc10,edc11,edc12,edc13,edc14,ec1,edp1,edp2,edp3,edp4,edp5,edp6,edp7,edp8,edp9,edp10\}$$

其中：edc_i 表示的箭头为分解意图关系，edp_i 表示的箭头为依赖意图关系，ec_i 表示的箭头为贡献意图关系。

节点字符集合 G_N 为

$$G_N=\{ng1,nt1,nt2,nt3,ng2,nt4,nt5,nt6,nt7,ng3,nt8,nt9,ng4,nt10,nt11,nt12,nt13,nt14,nt15,nt16,nt17\}。$$

源映射 s 和目标映射 t 为

$$s(edc1)=ng1,s(edc2)=ng1,s(edc3)=ng1,s(edc4)=ng2,s(edc5)=ng2,\ldots,$$

$$t(edc1)=nt1,t(edc2)=nt2,t(edc3)=nt3,t(edc4)=nt4,t(edc5)=nt5,\ldots。$$

根据以上定义，图 5 显示了 Web Payment 系统的形式化

图范畴模型。

表 1　Web Payment 系统的图范畴节点描述

Table 1　Node description of graph category for the Web Payment system

节点	节点描述
ng1	*Gain Goods Options*
ng2	*Online Payment*
ng3	*Provide Goods Options*
ng4	*Offer Payment Service*
nt1	*Search Items*
nt2	*Select Goods*
nt3	*Receive Options*
nt4	*Select Payment Instrument*
nt5	*Input Authentication Code*
nt6	*Receive Digital Receipt*
nt7	*Receive Payment Proof*
nt8	*Receive Search Requirement*
nt9	*Search Service*
nt10	*Initiate Payment Authorization*
nt11	*Offer Payment Instrument*
nt12	*Authorize Transfer*
nt13	*Complete Transfer*
nt14	*Send Digital Receipt*
nt15	*Receive Payment Authorization*
nt16	*Finalize Payment*
nt17	*Verify Available*

4.4　GRL 模型正确性验证

图 5 清晰的显示了功能方面的因果联系可以通过意图关系来刻画。根据定义 6，节点 $ng1$ 为 Web Payment 系统目标模型的初始对象，而节点 $nt1$、$nt2$、$nt3$、$nt4$、$nt5$、$nt6$、$nt8$、$nt9$、$nt10$、$nt11$ 为 Web Payment 系统目标模型的终止对象，存在多个射集合，其中的一个射集合 $G_{A1}=\{edp1:s(edp1)\to t(edp1)$，$edp2:t(edp1)\to t(edp2)$，$edp3:t(edp2)\to t(edp3)$，$edp3:t(edp2)\to t(edp3)$，$edp4:t(edp3)\to t(edp4)\ \ldots\}$，根据射集合，整个目标形式化模型系统存在着多条紧邻序列。主要包括：

$$Neighbor-S1=\{ng1\to ng3\to ng2\to ng4\to nt15\to nt17\to nt12\to nt16\to nt13\to nt14\to nt7\to nt6\}$$

$$Neighbor-S2=\{ng1\to ng3\to ng2\to nt4\}$$

$$Neighbor-S3=\{ng1\to ng3\to ng2\to nt5\}$$

$$Neighbor-S4=\{ng1\to ng3\to ng1\to nt1\}$$

$$Neighbor-S5=\{ng1\to ng3\to ng2\to ng4\to ng2\to ng3\ldots\}$$

……

这些紧邻序列描述系统的查找商品、下订单、订单支付等业务目标的实现过程。因此，需要利用形式化模型验证该业务目标模型中是否存在孤立的节点、所有紧邻序列是否存在闭环情况、以及全局目标与子任务之间的“分派”关系等性质。

根据第 3 节定义的正确性结构性质对该目标模型进行验证：

a）孤立节点的验证问题，以上紧邻序列覆盖了该模型中的所有节点，该模型的紧邻集合为 $\sum Neighbor-S=$ 。应用定理 2

$$\sum Neighbor-S=G_N\{ng1,ng2,ng3,ng4,nt1,nt2,nt3,nt4,nt5,nt6,nt7,nt8,nt9,nt10,nt11,nt12,nt13,nt14,nt15,nt16,nt17\}$$

表明该模型中的所有节点都不是孤立的，即该目标模型系统是连通的。

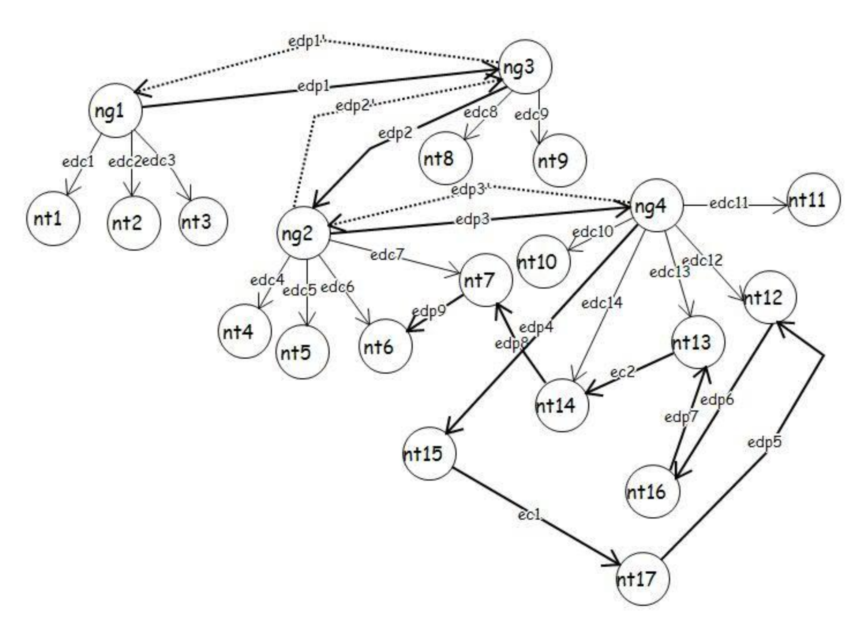


图 5　形式化 Web Payment 系统 GRL 模型的图范畴模型

Fig. 5　Graph category model by the formalized GRL model of the Web Payment

b）紧邻序列的闭环验证问题，应用定理 3，该目标模型系统中不存在无限循环执行的紧邻序列，表明该目标模型系统是没有闭环的。

c）全局目标与子任务的分派验证问题，应用定理 4，该目标模型系统中存在 gain goods options、online payment、provide goods options、offer payment service 四个全局目标。这四个全局目标都被分解为若干个子任务，这些子任务之间不存在依赖关系，且只有当所有子任务都完成，全局目标才能实现。以 offer payment service 为例，只有当 offer payment instrument、initiate payment authorization、authorize transfer、complete transfer 和 send digital receipt 这五个子任务都实现，该目标才能完整实现。否则，这五个子任务中任一任务没有

完成，则目标 Offer Payment Service 没有实现，说明在支付服务中出现了异常。因此，该目标模型满足“目标-分派”关系。

根据这三个正确性结构性质，可以验证图 4 所示的目标模型是正确的。

从语义角度上看，紧邻序列 *Neihgbor-S*1（图 5，粗箭头）是用户在 Web Payment 业务系统上进行的完整网上购物业务。由于定义了目标类型节点之间的双射性质，紧邻序列 *Neihgbor-S*4 表示用户对 Online Shopping Site 查询的商品结果不满意，进行的重新商品查询功能；紧邻序列 *Neihgbor-S*5 则表明用户在支付环节中出现异常或者用户主动放弃商品的支付。虽然在该图中还存在 *Neihgbor-S*2，*Neihgbor-S*3 等因果序列，但是这些序列可以通过领域专家和业务分析员的专业知识分析其语义，确定该因果序列是不正确的。因此，图 5 所示的所有正确紧邻序列可以覆盖 Web Payment 业务系统中的所有功能方面的特征。

5 结束语

本文针对业务目标模型的正确性验证问题，提出了扩展传统范畴理论，设计了图范畴方式形式化 GRL 目标模型的方法，定义了目标模型正确性验证的结构性质。该方法通过定义 GRL 模型的形式化语法结构和语义，设计形式化业务目标系统的结构，定义双射性质和目标系统的紧邻序列，设计目标系统的连通性、无闭环和“目标-分派”关系等结构性质对 GRL 目标模型进行正确性验证。

通过 Web Payment 实例演示，本文设计的射集合能够比较完整的描述目标模型中各节点之间的关系，通过形式化定义目标系统的初始对象和终止对象，设计的紧邻序列能够完整的描述业务目标模型中的业务功能。本形式化方法与 Popova 等人[11]的谓词方法、Diamantini 等人[14]的本体目标模型相比，本形式化方法对目标模型节点间关系的刻画具有一定的优势。

但文中的模型形式化目前仍由手工生成，且文中为了保障目标模型系统中的每个节点都能够被遍历，使得紧邻序列中存在大量的无效序列。因此，如何实现形式化的自动执行，以及如何进一步筛选出系统的有效序列，提高模型形式化的效率是下一步研究工作需要解决的主要问题。

参考文献：

[1] Jureta I J, Faulkner S, Schobbens P Y. Clear justification of modeling decisions for goal-oriented requirements engineering [J]. Requirements Engineering, 2008, 13(2): 87-115.

[2] Van Lamsweerde A. Goal-oriented requirements engineering: a guided tour [C]. //Proc of the 5th IEEE International Symposium on Requirements Engineering. Piscataway,NJ：IEEE Press, 2001: 249-262.

[3] Bernardo M, Inverardi P. Formal Methods for software architectures [C]//Lecture Notes in Computer Science. 2003.

[4] GRL [EB/OL]. http://www. cs. toronto. edu/km/GRL/.

[5] Amyot D. Introduction to the user requirements notation: learning by example [J]. Computer Networks, 2003, 42: 285-301.

[6] Mussbacher G, Ghanavati S, Amyot D. Modeling and analysis of URN goals and scenarios with jUCMNav [C]. //Proc of the 17th IEEE International Requirements Engineering Conference. Washington DC: IEEE Computer Society, 2009: 383-384.

[7] Meland P H, Paja E, Gjære E A, *et al.* Threat analysis in goal-oriented security requirements modelling [J]. International Journal of Secure Software Engineering, 2014, 5 (2): 1-19.

[8] Sabatucci L, Cossentino M, Susi A. A goal-oriented approach for representing and using design patterns [J]. Journal of Systems and Software, 2015, 110(12): 136-154.

[9] Laibinis L, Pereverzeva I, Troubitsyna E. Formal reasoning about resilient goal-oriented multi-agent systems[J]. Science of Computer Programming, 2017, 148 (11): 66-87.

[10] 张璇，王旭，李彤，等. 面向方面业务过程建模的正确性控制与检测 [J]. 计算机学报, 2018, 41(3): 521-544. (Zhang Xuan, Wang Xu, Li Tong, *et al.* Correctness control and detection in aspect-oriented business process modeling [J]. Chinese Journal of Computers, 2018, 41 (3): 521-544.)

[11] Popova V, Sharpanskykh A. Formal modelling of organisational goals based on performance indicators [J]. Data & Knowledge Engineering, 2011, 70: 335-364.

[12] Giachetti G, Marín B, López L, *et al.* Verifying goal-oriented specifications used in model-driven development processes [J]. Information Systems, 2017, 64(3): 41-62.

[13] Mendonça D F, Rodrigues G N, Ali R, *et al.* GODA: a goal-oriented requirements engineering framework for runtime dependability analysis [J]. Information and Software Technology, 2016, 80(12): 245-264.

[14] Diamantini C, Freddi A, Longhi S, *et al.* A goal-oriented, ontology-based methodology to support the design of AAL environments [J]. Expert Systems with Applications, 2016, 64(12): 117-131.

[15] 贾伟，华庆一，张敏军，等. 基于范畴论的用户界面模式语言 [J]. 计算机辅助设计与图形学学报，2017, 29(1): 79-89. (Jia Wei, Hua Qingyi, Zhang Minjun, *et al.* User interface pattern language based on category theory [J].Journal of Computer-Aided Design & Computer Graphics, 2017, 29(1): 79-89.)

[16] Barr M, Wells C. Category theory for computing science [M]. Upper Saddle River: Prentice-Hall, 2012.

[17] Fiadeiro J L. Categories for software engineering [M]. Berlin: Springer, 2005.

[18] Zhu M, Grogono P, Ormandjieva O, *et al.* Using category theory and data flow analysis for modeling and verifying properties of communications in the process-oriented language Erasmus [C]. //Proc of the 7th Conference on Computer Science and Software Engineering. 2014: 1-24.

[19] Ormandjieva O, Bentahar J, Huang J, *et al.* Modelling multi-agent systems with category theory [J]. Procedia Computer Science, 2015, 52: 538-545.

[20] Mylopoulos J, Chung L, Yu E. From object-oriented to goal-oriented requirements analysis [J]. Communications of the ACM, 1999, 42(1): 31-37.

[21] 刘春，黄冉冉，韩道军. 基于目标的信息物理融合系统事件模型的分析[J]. 计算机科学, 2017, 44(4): 100-103. (Liu Chun, Huang Ranran, Han Daojun. Goal oriented approach for analayzing event model of cyber-physical systems [J]. Computer Science, 2017, 44(4): 100-103.)

[22] Li Zonghua, Zhou Xxiaofeng, Gu Aihua, *et al.* A complete approach for CIM modelling and model formalizing [J]. Information and Software Technology, 2015, 65 (C): 39-55.

[23] W3C, Web Payments Use Cases 1. 0[EB/OL]. [2015-07-30]. https://www. w3. org/TR/web-payments-use-cases/.